Crv napada Linksysove routere

Ako posjedujete male bežične routere tvrtke Linksys, možda ste primijetili da vam je u zadnje vrijeme mrežni promet usporen. To bi moglo značiti da je vaš uređaj inficiran i da za račun nepoznatog napadača skenira mrežu i širi infekciju na druge slične uređaje.

Napad počinje upitom na port 8080 na kojem se odaziva HNAP protokol (Home Network Administration Protocol). Radi se o sučelju koje omogućava ISP-u udaljenu administraciju tih malih uređaja. I sami možete provjeriti da li je vaš uređaj ranjiv, tako što ćete sa svog Linuxa pokrenuti slijedeću naredbu:

```
echo "GET /HNAP1/ HTTP/1.1\r\nHost: test\r\n\r\n" | nc 192.168.1.1 8080
```

Ovdje se podrazumijeva da je router na tipičnoj adresi 192.168.1.1. Ako dobijete odgovor, vaš je uređaj vjerojatno ranjiv na ovaj napad. Mrežni crv će u odgovoru potražiti sijedeće retke:

```
<ModelName>E2500</ModelName>
<FirmwareVersion>1.0.07 build 1</FirmwareVersion>
```

Ranjiva je, navodno, samo E serija Linksysovih uređaja. Kad ustanovi da je uređaj ranjiv, crv će sa inficiranog uređaja na novotkriveni isporučiti kod exploita, nakon čega će i taj uređaj skenirati mrežu i širiti infekciju. Iako se zasad o ovom zloćudnom softveru govori kao o crvu, mogao bi se iskoristiti za stvaranje botneta.

Crva proučavaju u SANS-u, čiji je tehnički direktor Johannes B. Ullrich na svom blogu objavio što su dosad otkrili. Navodno su u exploitu ukodirane IP adrese na koje se crv nastoji proširiti, a koje pripadaju nekim poznatim ISP-ovima. Mi ćemo se možda ovog puta provući jer smo mala meta, međutim nije nikakakv problem modificirati kod i dodati adrese domaćih ISP-ova. U trenutku objave članka u jednoj našoj srednjoj školi pokušavaju otkriti zašto im je bežična mreža toliko usporena da profesori imaju problema spojiti se sa svojih tableta. Ne znamo još rezultat istrage, ali svakako bi trebalo provjeriti radi li se o ovom crvu.

Više možete saznati na stranicama SANS [1]-a, te iz članka u časopisu Ars technica [2].

Ako vas zanima i HNAP, informacije su dostupne ovdje [3].

pon, 2014-02-17 07:06 - Aco Dmitrović**Vijesti:** Sigurnosni propusti [4]
Kategorije: Sigurnost [5]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

Source URL: https://sysportal.carnet.hr/node/1354

Links
[1] https://isc.sans.edu/diary/Linksys+Worm+Captured/17630
[2] http://arstechnica.com/security/2014/02/bizarre-attack-infects-linksys-routers-with-self-replicating-malware/
[3] http://www.cisco.com/web/partners/downloads/guest/hnap_protocol_whitepaper.pdf
[4] https://sysportal.carnet.hr/taxonomy/term/14
[5] https://sysportal.carnet.hr/taxonomy/term/30

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr